

Оглавление

Составители	16
Авторы	16
Рецензенты	18
Введение	19
Для кого предназначена книга	19
Структура издания	19
Как получить максимальную пользу от этой книги	21
Условные обозначения	21
От издательства	22
Глава 1. Установка и настройка Kali Linux	23
Технические условия	23
Категории инструментов Kali Linux	23
Загрузка Kali Linux	26
Начинаем работать с Kali Linux	29
Запуск Kali Linux с Live DVD	29
Установка на жесткий диск	30
Установка Kali на USB	43
Настройка виртуальной машины	45
Гостевые дополнения VirtualBox	45
Настройка сети	47
Обновление Kali Linux	51
Настройка Kali Linux AMI в облаке Amazon AWS	52

Резюме.....	62
Вопросы	63
Дополнительные материалы	63
Глава 2. Создание испытательной лаборатории.....	64
Технические требования.....	64
Физическая или виртуальная?.....	65
Настройка Windows на виртуальной машине.....	65
Установка уязвимых серверов.....	71
Настройка Metasploitable 2 на виртуальной машине.....	71
Настройка Metasploitable 3 на виртуальной машине.....	73
Предварительная настройка Metasploitable 3.....	77
Установка и настройка BadStore на виртуальной машине	78
Установка дополнительных инструментов в Kali Linux	84
Сетевые сервисы в Kali Linux	85
HTTP.....	85
MySQL.....	86
SSH.....	87
Дополнительные лаборатории и ресурсы.....	88
Резюме.....	90
Вопросы	91
Дополнительные материалы	91
Глава 3. Методология тестирования на проникновение	92
Технические условия	92
Методология тестирования на проникновение	92
Руководство по тестированию OWASP	93
PCI-руководство по тестированию на проникновение	94
Стандартное проведение тестов на проникновение	95
NIST 800-115	95
Руководство по методологии тестирования безопасности с открытым исходным кодом	96
Фреймворк: общее тестирование на проникновение.....	96
Разведка.....	97
Сканирование и перечисление.....	98
Получение доступа.....	104

Повышение привилегий	109
Поддержание доступа	109
Заметание следов	110
Составление отчета	110
Резюме	111
Глава 4. Получение отпечатка и сбор информации.....	112
Разведка по открытым источникам	113
Использование общих ресурсов.....	113
Запрос сведений о регистрации домена	114
Анализ записей DNS	115
Получение имени хоста	116
dig: техники разведывания DNS	117
DMitry: магический инструмент для сбора информации	118
Maltego: графическое отображение собранной информации.....	120
Получение сведений о сетевой маршрутизации.....	127
tcptracroute.....	127
tctrace	128
Используем поисковик.....	129
Взлом базы данных Google (GHDB).....	131
Metagoofil	133
Автоматизированные инструменты для снятия отпечатков и сбора информации.....	137
Devploit.....	137
RedHawk v2.....	140
Использование Shodan для поиска подключенных к Интернету устройств	142
Blue-Thunder-IP-локатор.....	144
Резюме	147
Вопросы	148
Дополнительные материалы	148
Глава 5. Методы сканирования и уклонения	149
Технические условия	149
Начинаем с обнаружения цели.....	149

Идентификация целевой машины.....	150
ping.....	150
fping.....	153
hping3.....	155
Получение отпечатков ОС.....	158
Введение в сканирование портов.....	161
Изучаем протокол TCP/IP.....	161
Тонкости форматов сообщений TCP и UDP.....	163
Сетевой сканер.....	166
Что такое Nmap.....	167
Спецификация цели.....	169
Параметры сканирования TCP.....	171
Сканирование UDP.....	173
Спецификация порта Nmap.....	173
Параметры вывода Nmap.....	175
Параметры синхронизации.....	177
Полезные параметры Nmap.....	178
Nmap для сканирования IPv6.....	181
Сценарный движок Nmap.....	182
Параметры Nmap для обхода идентификаторов брандмауэра.....	186
Сканирование с Netdiscover.....	187
Автоматическое сканирование с помощью Striker.....	188
Анонимность с помощью Nipe.....	191
Резюме.....	193
Вопросы.....	193
Дополнительные материалы.....	194
Глава 6. Сканирование уязвимостей.....	195
Технические требования.....	196
Типы уязвимостей.....	196
Локальные уязвимости.....	196
Удаленная уязвимость.....	197
Систематизация уязвимостей.....	197

Автоматическое сканирование уязвимостей	198
Nessus 7	198
OpenVAS	206
Сканирование уязвимостей Linux с помощью Lynis.....	212
Сканирование и перечисление уязвимостей с помощью SPARTA.....	217
Резюме	222
Вопросы	223
Дополнительные материалы	223
Глава 7. Социальная инженерия	224
Технические условия	225
Моделирование психологии человека	225
Процесс атаки	225
Методы атаки	226
Подражание.....	227
Взаимный обмен.....	227
Влияние авторитета	228
Использование жадности.....	228
Налаживание социальных взаимоотношений.....	229
Сила любопытства.....	229
Инструменты социальной инженерии.....	229
Анонимная USB-атака	231
Сбор учетных данных.....	235
Вредоносный Java-апплет	238
Резюме	242
Глава 8. Целевая эксплуатация	243
Исследование уязвимости.....	243
Хранилища уязвимостей и эксплойтов	245
Расширенный инструментарий эксплуатации.....	246
MSFConsole	247
MSFCLI	249
Ninja 101 drills	251
Сценарий 1	251

Сценарий 2	252
Сценарий 3	255
Написание модулей эксплойта	263
Резюме	267
Глава 9. Повышение привилегий и поддержание доступа.....	268
Технические требования.....	268
Повышение привилегий.....	268
Локальная эксплуатация	269
Инструменты подбора пароля	273
Инструменты для автономной атаки	274
Инструменты онлайн-атаки	281
Поддержание доступа	287
Бэкдор для входа в операционную систему	287
Резюме	292
Глава 10. Тестирование веб-приложений	293
Технические требования.....	293
Веб-анализ	294
nikto	294
OWASP ZAP	296
Burp Suite.....	299
Прокси-сервер Paros.....	309
W3AF	311
WebScarab.....	314
Межсайтовые сценарии.....	316
Тестирование XSS	316
SQL-инъекция	320
Инструкция для SQL-инъекции.....	321
Автоматическая SQL-инъекция	323
Выполнение команд, обход каталогов и включение файлов	326
Обход каталогов и включение файлов	327
Выполнение команд.....	330
Резюме	334
Дополнительные материалы	335

Глава 11. Тестирование беспроводных сетей на проникновение	336
Технические требования.....	337
Беспроводная сеть.....	337
Обзор стандарта IEEE 802.11	337
Протокол безопасности беспроводных локальных сетей.....	338
Защищенный доступ Wi-Fi (WPA)	339
Разведка в беспроводной сети.....	340
Антенны.....	341
Iwlist	341
Kismet.....	342
WAIDPS.....	344
Инструменты тестирования беспроводной сети	346
Aircrack-ng.....	347
PixieWPS	359
Wifite	359
Fern Wifi Cracker.....	361
Атака «злой двойник»	364
После взлома.....	368
MAC-спуфинг	369
Устойчивость.....	370
Анализ беспроводного трафика.....	372
Анализ WLAN-трафика.....	372
Пассивный анализ	376
Резюме.....	380
Глава 12. Мобильное тестирование на проникновение с Kali NetHunter	381
Технические требования.....	381
Kali NetHunter	381
Развертывание.....	382
Развертывание сети.....	382
Развертывание беспроводной сети	382
Развертывание узла.....	383
Установка Kali NetHunter	383
Значки NetHunter	384

Инструменты NetHunter	386
Nmap	386
Metasploit	388
Преобразователь MAC	391
Сторонние приложения Android	392
Приложение NetHunter Terminal	392
DriveDroid	393
USB-клавиатура	393
Shodan	394
Router Keygen	394
cSploit	395
Беспроводные атаки	396
Беспроводное сканирование	397
WPA/WPA2-взлом	398
WPS-взлом	399
Атака «злой двойник»	401
NID-атаки	406
Резюме	409
Вопросы	410
Дополнительные материалы	410
Глава 13. PCI DSS: сканирование и тестирование на проникновение	411
PCI DSS v3.2.1, требование 11.3	412
Определение области испытания на проникновение PCI DSS	413
Сбор требований клиентов	415
Создание формы требования заказчика	415
Подготовка плана испытаний	416
Контрольный список плана тестирования	418
Границы профилирования теста	419
Определение бизнес-целей	420
Управление проектами и планирование	421
Инструменты для выполнения теста на проникновение в платежные системы	422
Резюме	424
Вопросы	424
Дополнительные материалы	424

Глава 14. Инструменты для создания отчетов о тестировании	
на проникновение	426
Технические условия	427
Документация и проверка результатов	427
Типы отчетов.....	428
Исполнительный доклад.....	429
Отчет для руководства.....	429
Технический отчет.....	430
Отчет о тестировании проникновения в сеть.....	431
Подготовка презентации	432
Процедуры после тестирования	433
Использование структуры Dradis для составления отчетности по тестированию на проникновение.....	434
Инструменты отчетности по тестированию на проникновение	439
Faraday IDE.....	439
MagicTree.....	440
Резюме.....	441
Вопросы	441
Дополнительные материалы	442
Ответы на вопросы	443
Глава 1	443
Глава 2	443
Глава 4	443
Глава 5	444
Глава 6	444
Глава 12.....	445
Глава 13.....	445
Глава 14.....	445